

Building Digital Trustworthiness at the Utah State Archives



The Golden Rule of Digital Preservation

“Striving to better, oft
we mar what's well.”

- Shakespeare in *King
Lear*

The Golden Rule of Digital Preservation

“...the best is the enemy of the good.”
- Voltaire

The Golden Rule of Digital Preservation

“If you never miss a plane,
you're spending too much
time at the airport.”

- George Stigler

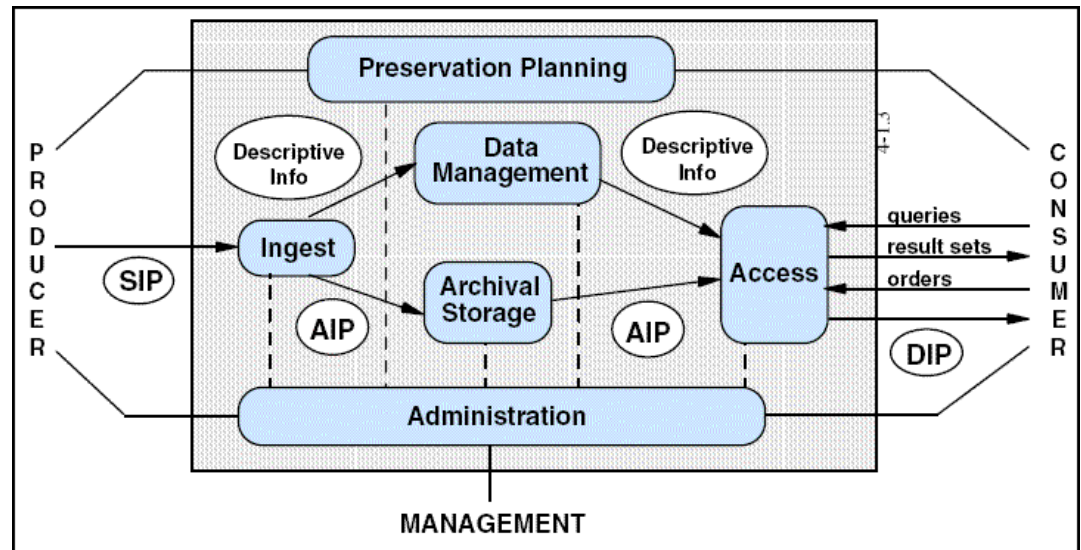
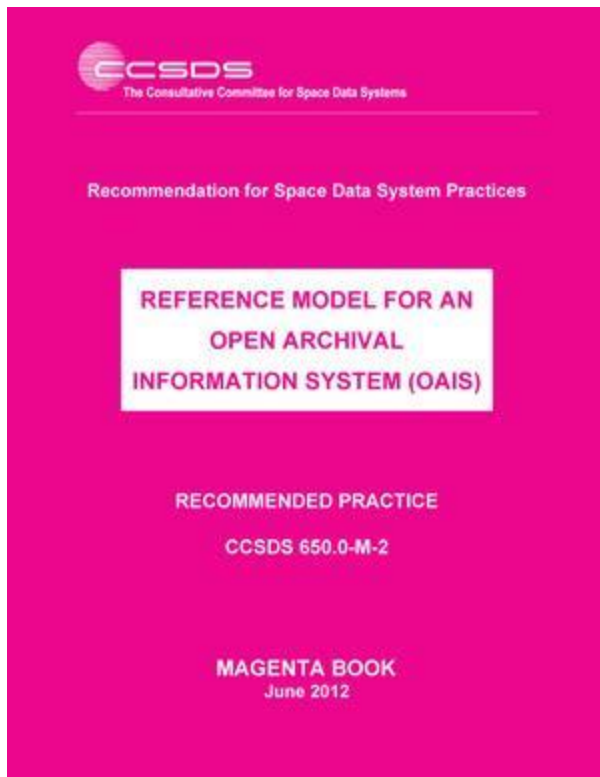
Topics for Today

1. What is a trusted digital repository, and why should you care?
2. How is the Utah State Archives building systems and programs that embrace digital trustworthiness?
3. How can other governmental entities assist us in building a trustworthy electronic records preservation program statewide?

Trusted Digital Repositories

- Foundation rests on the core archival principles of maintaining integrity of digital objects over time, and providing ongoing access to those materials in perpetuity.



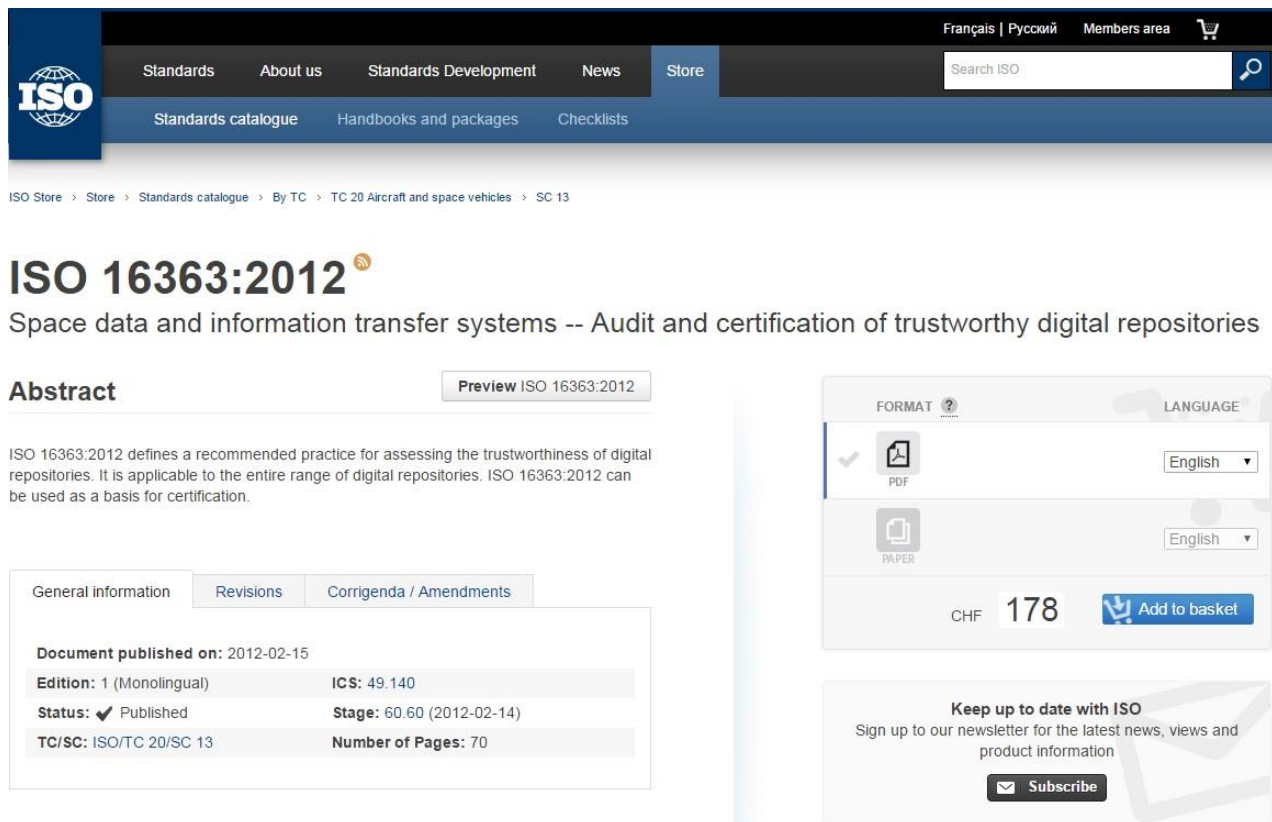


<http://public.ccsds.org/publications/archive/650x0m2.pdf>

Trusted Digital Repositories

- The standards for certification as a trusted digital repository have evolved heavily over the last 20 years.
- TRAC (Trusted Repositories Audit and Certification) emerged as the gold standard beginning in 2007. However, it has been superseded by the even more comprehensive ISO standards 16363 (2012) and 16919 (2014).

Trusted Digital Repositories



The screenshot shows the ISO website interface for the ISO 16363:2012 standard. The top navigation bar includes links for Standards, About us, Standards Development, News, and Store. A search bar is located on the right. Below the navigation bar, the breadcrumb trail reads: ISO Store > Store > Standards catalogue > By TC > TC 20 Aircraft and space vehicles > SC 13.

ISO 16363:2012

Space data and information transfer systems -- Audit and certification of trustworthy digital repositories

Abstract

ISO 16363:2012 defines a recommended practice for assessing the trustworthiness of digital repositories. It is applicable to the entire range of digital repositories. ISO 16363:2012 can be used as a basis for certification.

[Preview ISO 16363:2012](#)

General information	
Document published on: 2012-02-15	
Edition: 1 (Monolingual)	ICS: 49.140
Status: Published	Stage: 60.60 (2012-02-14)
TC/SC: ISO/TC 20/SC 13	Number of Pages: 70

FORMAT LANGUAGE

☒ PDF English

☐ PAPER English

CHF 178 [Add to basket](#)

Keep up to date with ISO
Sign up to our newsletter for the latest news, views and product information
[Subscribe](#)

http://www.iso.org/iso/catalogue_detail.htm?csnumber=56510

Trusted Digital Repositories



ISO 16919:2014

Space data and information transfer systems -- Requirements for bodies providing audit and certification of candidate trustworthy digital repositories

Abstract

[Preview ISO 16919:2014](#)

ISO 16919:2014 is meant primarily for those setting up and managing the organization performing the auditing and certification of digital repositories.

It should also be of use to those who work in or are responsible for digital repositories seeking objective measurement of the trustworthiness of their repository and wishing to understand the processes involved.

The main purpose is to define a CCSDS Recommended Practice (and ISO International Standard) on which to base the operations of the organization(s) which assess the trustworthiness of digital repositories using ISO 16363 and provide the appropriate certification. ISO 16919:2014 specifies requirements for bodies providing audit and certification of digital repositories, based on the metrics contained within ISO/IEC 17021 and CCSDS 652.0-M-1/ISO 16363. It is primarily intended to support the accreditation of bodies providing such certification.

FORMAT ?		LANGUAGE
<input checked="" type="checkbox"/>		English
<input type="checkbox"/>		English
CHF 118		Add to basket

Keep up to date with ISO
Sign up to our newsletter for the latest news, views and product information

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57950

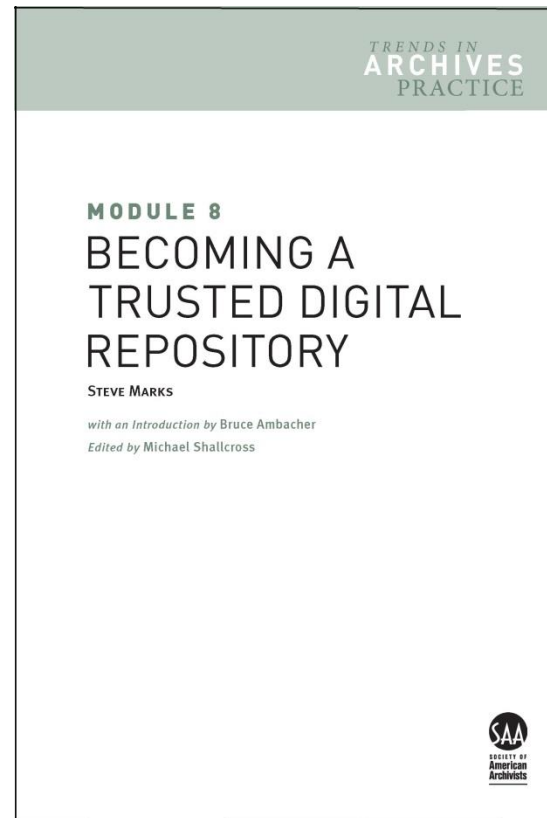
Trusted Digital Repositories

WHY “CERTIFY?”

- ◉ Simply put, the certification and audit standards for becoming a Trusted Digital Repository provide a template and checklist that any organization can utilize in modeling their digital preservation program(s).
- ◉ Very likely that most of the TRAC standards won't apply, particularly to smaller organizations. However, it is still a wonderful tool for helping to determine where you are, where you want to be, and potential strategies for getting there.
- ◉ Also provides the benefit of ensuring that programs and projects are built upon internationally accepted standards for digital preservation.

Trusted Digital Repositories

Core Elements
of the Trusted
Digital
Repository
Standard



<http://saa.archivists.org/store/module-8-becoming-a-trusted-digital-repository/4679/>

Trusted Digital Repositories

SECTION 3: Organizational Infrastructure

- Governance and Organization Viability
- Organization Structure and Staffing
- Procedural Accountability and Preservation Policy Framework
- Financial Sustainability
- Contracts, Licenses and Liabilities

Trusted Digital Repositories

SECTION 4: Digital Object Management

- Ingest: Content Acquisition
- Ingest: Creating ALPs
- Preservation Planning
- ALP Preservation
- Information Management
- Access Management

Trusted Digital Repositories

SECTION 5: Infrastructure and Security Risk Management

- Technical Infrastructure Risk Management
- Security Risk Management

Building Digital Trust at the Utah State Archives

TRAC [Home](#) [Responsibilities](#) [About](#) [Login](#)

TRAC Review: Process and Progress

This page provides an overview of an organization's efforts to document its evidence for meeting the requirements of the CCSDS Audit and Certification of Trustworthy Digital Repositories [checklist](#) that was approved as ISO 16363 and is based on Trustworthy Repositories Audit and Certification (TRAC). Criteria and Checklist that was released in January 2007. A TRAC review is a self-assessment method for an organization to demonstrate good practice and conformance as a trusted digital repository to its designated communities and prepare for a peer review or other external audit. In many organizations, responsibilities for TRAC compliance are distributed throughout the organization, with specific units and committees having certain responsibilities for each requirement.

Responsibilities

Each entity is assigned a role for each requirement using the RACI responsibility assignment matrix. The RACI Matrix describes participation by various organizational roles in completing tasks for a project. RACI is especially useful in clarifying roles in projects and processes requiring distributed responsibilities. See the [Responsibilities for TRAC](#) page for more information on RACI responsibilities, and a listing of units and committees that have roles in TRAC conformance.

Requirements

Each TRAC requirement has its own page. Sub- and Sub-sub requirements are referred to on the relevant high-level requirement page. Current compliance with TRAC requirements is assessed on a rating system from 0 to 4 (see example: [SGDS report](#), page 14):

- 4 = fully compliant - the repository can demonstrate that has comprehensively addressed the requirement
- 3 = mostly compliant - the repository can demonstrate that it has mostly addressed the requirement and is on working on full compliance
- 2 = half compliant - the repository has partially addressed the requirement and has significant work remaining to fully address the requirement
- 1 = slightly compliant - the repository has something in place, but has a lot of work to do in addressing the requirement
- 0 = non-compliant or not started - the repository has not yet addressed the requirement or has not started the review of the requirement

Any group in the organization that is involved in defining policy and practice should update the status of relevant requirements. When listing evidence, please include sufficient information for reviewers to get to the cited evidence (e.g., a document title, date, a link) and note the name of the group or department that is adding an entry to the evidence. Addressing the requirement along with the date of the annotations (e.g., [Right Management group, 2/13/2013]). For additional guidance, please see the [Responsibilities for TRAC](#) page.

Status

The summary below reflects this sequence of status levels.

- Accepted – the evidence provided has been accepted as sufficient for this review round
- Ready for review – the Responsible group has completed its work and the evidence is ready for review
- In progress – the Responsible group is in the process of compiling or generating relevant evidence
- Not started – no evidence or information has been provided yet

[Printer-friendly version](#)

Status Summary

Section	Total Requirements *	Average Compliance Rating
3. Organizational Infrastructure	25	0.1200
4. Digital Object Management	60	2.5500
5. Infrastructure and Security Risk Management	24	0.0417

* The total number of requirements include sub-requirements and sub-sub-requirements for which TRAC provides a basis for a compliance rating.

The TRAC Review Tool (developed by Nancy McGovern) is a good first step in assessing where your digital program is, and where it needs go.

TRAC REVIEW: www.dpworkshop.org/trac

Building Digital Trust at the Utah State Archives

TRAC		
Home	Responsibilities	About Login
Requirement Status		
3.1 Governance and Organizational Viability	Compliance Rating	Status
3.1.1 Mission statement	0	Not started
3.1.2 Preservation Strategic Plan	0	Not started
3.1.2.1 Succession, contingency, and/or escrow plans	0	Not started
3.1.2.2 Organizational environment	0	Not started
3.1.3 Collection Policy	0	Not started
3.2 Organizational Structure and Staffing	Compliance Rating	Status
3.2.1 Adequate staffing	0	Not started
3.2.1.1 Established duties	0	Not started
3.2.1.2 Number of staff	0	Not started
3.2.1.3 Professional development	0	Not started
3.3 Procedural Accountability and Preservation Policy Framework	Compliance Rating	Status
3.3.1 Designated Community	0	Not started
3.3.2 Preservation Policies	0	Not started
3.3.2.1 Ongoing development of Preservation Policies	0	Not started
3.3.3 History of changes	0	Not started
3.3.4 Transparency and accountability	0	Not started
3.3.5 Information integrity measurements	3	In progress
3.3.6 Self-assessment and external certification	0	Not started

Building Digital Trust at the Utah State Archives

UTAH STATE ARCHIVES AND RECORDS SERVICE

Trustworthy Repositories Audit and Certification (TRAC) Review

Version 1.0

James Kichas
6/9/2015

This record documents the Utah State Archives and Records Service efforts to document its evidence for meeting the requirements of the CCSDS Audit and Certification of Trustworthy Digital Repositories checklist that was approved as ISO 16363 in 2012, and is based on Trustworthy Repositories Audit and Certification (TRAC): Criteria and Checklist that was released in January 2007. A TRAC review is a self-assessment method for an organization to demonstrate good practice and conformance as a trusted digital repository to its designated communities and prepare for a peer review or other external audit.

Table of Contents and Compliance Rating/Status Tracking

Section	Compliance Rating	Status	Page(s)
3.1 Governance and Organizational Viability			
3.1.1 Mission Statement	R	4	
3.1.2 Preservation Strategic Plan	R	3 or 4	
3.1.2.1 Succession, Contingency, and/or Escrow Plans	0	N	
3.1.2.2 Organizational Environment	0	N	
3.1.3 Collection Policy	0	N	
3.2 Organizational Structure and Staffing			
3.2.1 Adequate Staffing	0	N	
3.2.1.1 Established Duties	0	N	
3.2.1.2 Number of Staff	0	N	
3.2.1.3 Professional Development	0	N	
3.3 Procedural Accountability and Preservation Policy Framework			
3.3.1 Designated Community	0	N	
3.3.2 Preservation Policies	0	N	
3.3.2.1 Ongoing Development of Preservation Policies	0	N	
3.3.3 History of Changes	0	N	
3.3.4 Transparency and Accountability	0	N	
3.3.5 Information Integrity Measurements	0	N	
3.4 Financial Sustainability			
3.4.1 Business Planning Processes	0	N	
3.4.2 Financial Practices and Procedures	0	N	
3.4.3 Financial Analysis and Reporting	0	N	
3.5 Contracts, Licenses and Liabilities			
3.5.1 Contracts or Deposit Agreements	0	N	
3.5.1.1 Preservation Rights	0	N	
3.5.1.2 Agreements with Depositors	0	N	
3.5.1.3 Preservation Responsibility	0	N	
3.5.1.4 Liability and Challenges	0	N	
3.5.2 Intellectual Property Rights	0	N	
4.1 Ingest: Acquisition of Content			
4.1.1 Content Information and Information Properties	0	N	
4.1.1.1 Identification of Information Properties	0	N	
4.1.1.2 Record of Content Information and Information Properties	0	N	
4.1.2 Content Information Specifications	0	N	

Building Digital Trust at the Utah State Archives



Archives Storage Solutions Technical Final Proposal

Prepared by: Randy Spainhower and Joe Tripp

This is a final proposal for Archives Storage needs in FY 2016 and on. Each Storage Space outlined in the Archives Data Storage Business Analysis (Prepared by Gerry Satterlee) is discussed in the subsequent sections:

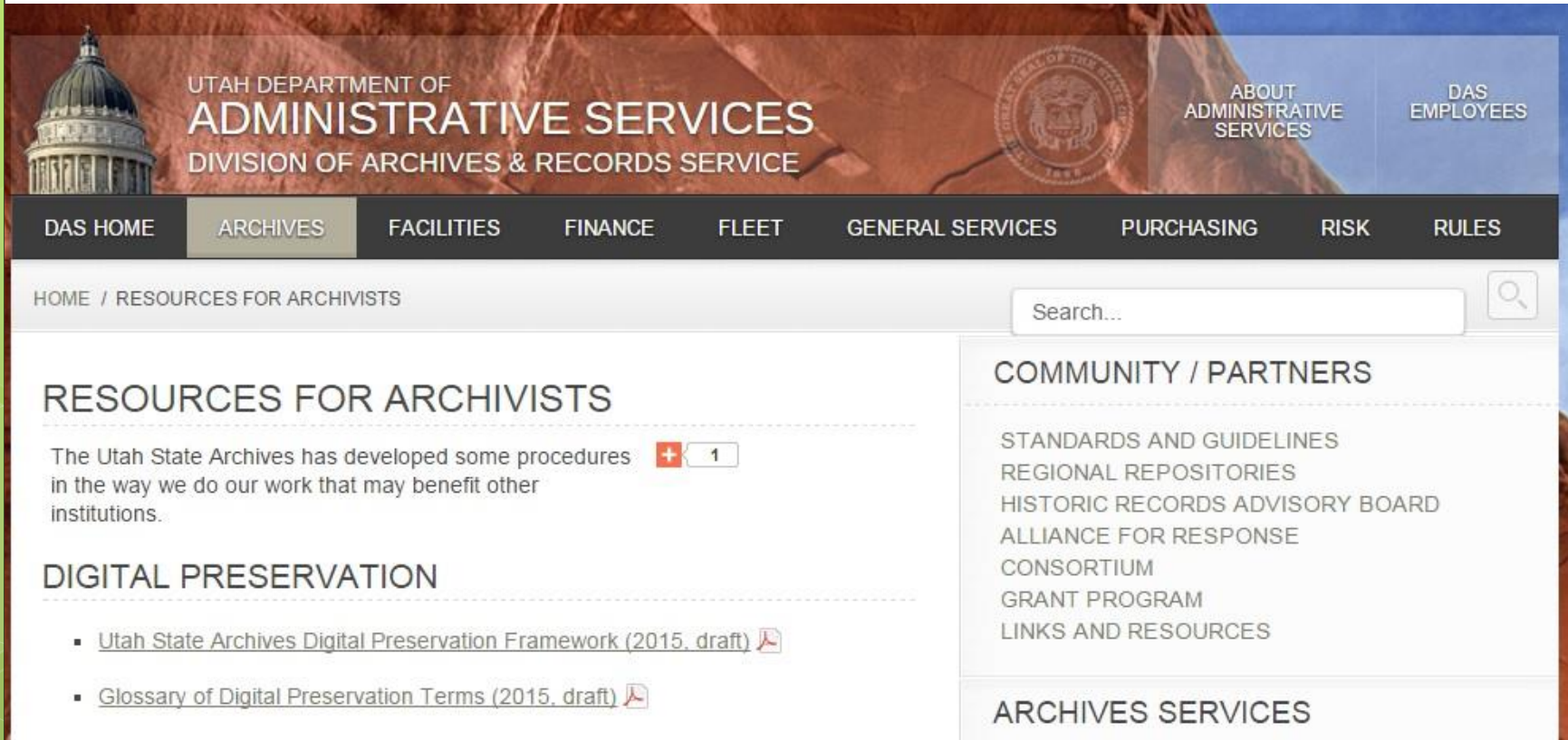
Quarantine Store

As Archives acquires records they first store them in a Quarantine space for 30 days. Right now they are using external hard drives for this purpose. It is our recommendation that they continue with this practice as this area really can be "quarantined" by storing the external hard drive unconnected for 30 days. Plus they have a second copy of the data from the initial submission.

Local Processing Store

Archives has need for a place to put submission data after it has been quarantined for 30 days.

Building Digital Trust at the Utah State Archives



The screenshot displays the Utah State Archives website. The header features the Utah Department of Administrative Services logo and the Division of Archives & Records Service. A navigation bar includes links such as DAS HOME, ARCHIVES, FACILITIES, FINANCE, FLEET, GENERAL SERVICES, PURCHASING, RISK, and RULES. The main content area is titled 'RESOURCES FOR ARCHIVISTS' and includes a search bar, a list of resources, and a sidebar with 'COMMUNITY / PARTNERS' and 'ARCHIVES SERVICES' sections.

UTAH DEPARTMENT OF
ADMINISTRATIVE SERVICES
DIVISION OF ARCHIVES & RECORDS SERVICE

ABOUT
ADMINISTRATIVE
SERVICES


DAS
EMPLOYEES

DAS HOME ARCHIVES FACILITIES FINANCE FLEET GENERAL SERVICES PURCHASING RISK RULES



HOME / RESOURCES FOR ARCHIVISTS

Search...

RESOURCES FOR ARCHIVISTS

The Utah State Archives has developed some procedures  1 in the way we do our work that may benefit other institutions.

DIGITAL PRESERVATION

- Utah State Archives Digital Preservation Framework (2015, draft) 
- Glossary of Digital Preservation Terms (2015, draft) 

COMMUNITY / PARTNERS

- STANDARDS AND GUIDELINES
- REGIONAL REPOSITORIES
- HISTORIC RECORDS ADVISORY BOARD
- ALLIANCE FOR RESPONSE
- CONSORTIUM
- GRANT PROGRAM
- LINKS AND RESOURCES

ARCHIVES SERVICES

<http://archives.utah.gov/community/archivistresources.html>

Building Digital Trust at the Utah State Archives

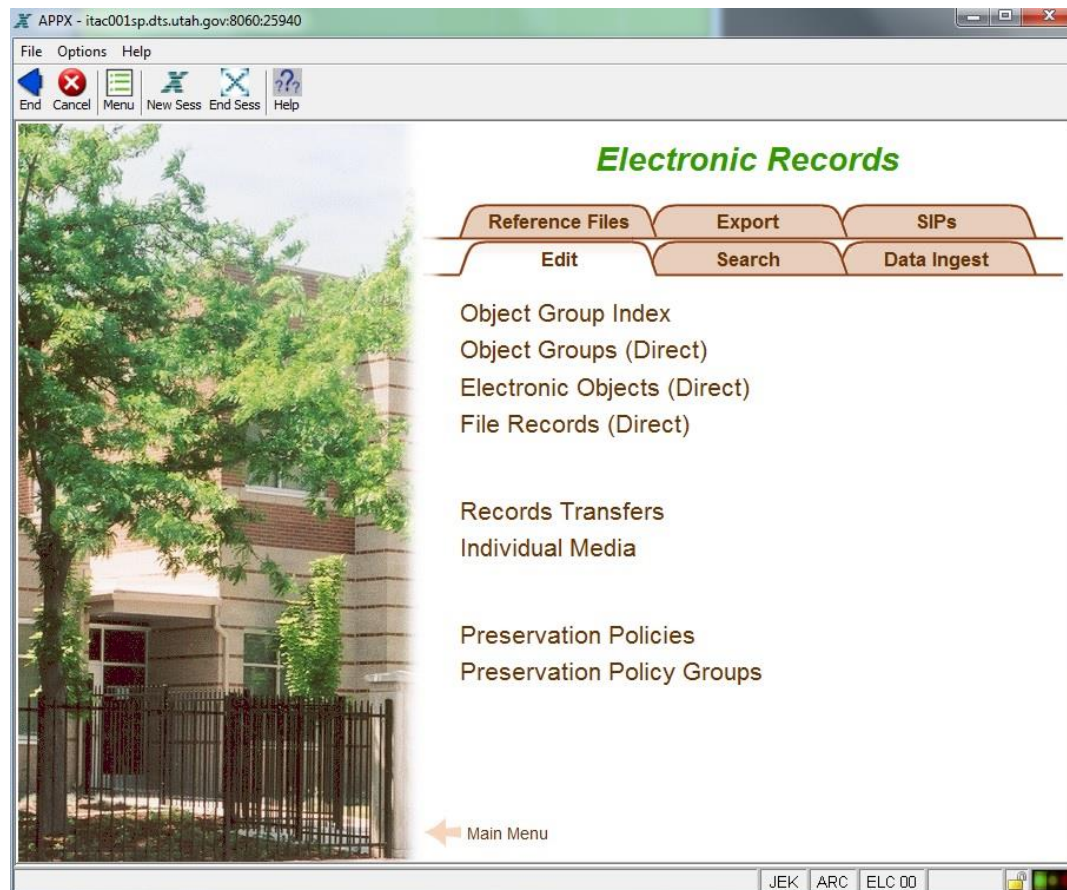
Digital Preservation Framework

Utah State Archives and Records Service

1. Purpose

This Digital Preservation Framework formalizes the Utah State Archive's commitment to the long-term preservation of its diverse and extensive range of digital resources, thereby assuring enduring access to these resources. This document outlines the Archive's approach to the preservation of digital resources and the associated information used to effectively manage these resources.

Building Digital Trust at the Utah State Archives



Building Digital Trust at the Utah State Archives

2015

Utah State Archives and
Records Service



[ELECTRONIC RECORDS POLICIES AND PROCEDURES (DRAFT VERSION 1.0)]

This document attempts to clearly define the pertinent policies and procedures adopted by the Utah State Archives and Records Service to ensure the proper transfer of electronic records to the repository and appropriate long term preservation in the repository's content management system.

□

Utah State Archives and Records Service Electronic Record Policies & Procedures Table of Contents

Part 1 – Governmental Entities and Electronic Records Submission and Acquisition

- 1.1 Submission Agreement Policy
 - 1.1.1 Submission Agreement Form Procedures
- 1.2 Acceptable Formats Policy
 - 1.2.1 File Formats Overview
 - 1.2.2 ICPR File Format Recommendations
 - 1.2.3 Recommended and Acceptable File Formats for Transfer to the Utah State Archives
 - 1.2.4 Encryption Policy
 - 1.2.4.1 Policy for Unencrypted Materials Entering Archives Custody
 - 1.2.4.2 Policy for Unencrypted Materials Entering Reformatting Section Custody
 - 1.2.4.3 Policy for Unencrypted Materials Distributed by the Archives Research Center
 - 1.2.4.4 Policy for Proprietary Archives Materials
- 1.3 SIP Creation and Validation Policy
 - 1.3.1 Before Transfer
 - 1.3.2 Bagit Procedures
 - 1.3.3 Immediately After Transfer
- 1.4 Acceptable Transfer Methods Policy
 - 1.4.1 Email
 - 1.4.2 Cloud Storage
 - 1.4.2.1 Google Drive
 - 1.4.2.2 Dropbox
 - 1.4.3 FTP Transfer
 - 1.4.4 Transfer of physical media
 - 1.4.4.1 Hard Drives
 - 1.4.4.2 CD/DVD
 - 1.4.4.3 Flash Drives
- 1.5 Archives Initiated Acquisition Policy
 - 1.5.1 Procedures for Obtaining Electronic Records from Open Records Portal
 - 1.5.2 Procedures for Harvesting Electronic Records Directly from the Web
 - 1.5.3 Procedures for Archives Initiated Acquisition of Government Employee Email

Part 2 – SIP Creation and Ingest

- 2.1 Accepting and Validating SIPs
 - 2.1.1 Quarantine Procedure
 - 2.1.2 Actions For When Validation Fails
- 2.2 Appraising and Weeding SIPs

E-Record Policies and Procedures (Ver. 1.0)

Building Digital Trust at the Utah State Archives

1.1.1 Submission Agreement Form Procedures

Procedures:

1.2 Acceptable Formats Policy

Policy Statement:

The Utah State Archives requires certain acceptable file formats to best ensure long-term preservation. File formats are the mechanism by which different types of digital information are encoded and stored. They are typically identified by their filename extension (e.g. .pdf, .jpg), allocated by the software that created the file. And this specific characteristic influences access to the content of the file, should the end-users have systems and software with the right technical abilities or dependencies to successfully open, access, use the content or not.

Some formats present greater risks to the continued accessibility of records than others. For example, when companies develop a file format, they can choose to keep the code closed (proprietary) or allow others to access it (open, non-proprietary). Open formats are less at risk of becoming inaccessible; with an open, published specification, anyone can develop a tool to open those files in the future if the original software becomes unavailable. Very common file formats (such as Microsoft formats), even if proprietary, are also at less risk of becoming inaccessible due to market demand.

Building Digital Trust at the Utah State Archives



<http://www.bpexchange.org/>



<http://www.statearchivists.org/seri/PERTTS/index.htm>



<http://www2.archivists.org/prof-education/das>

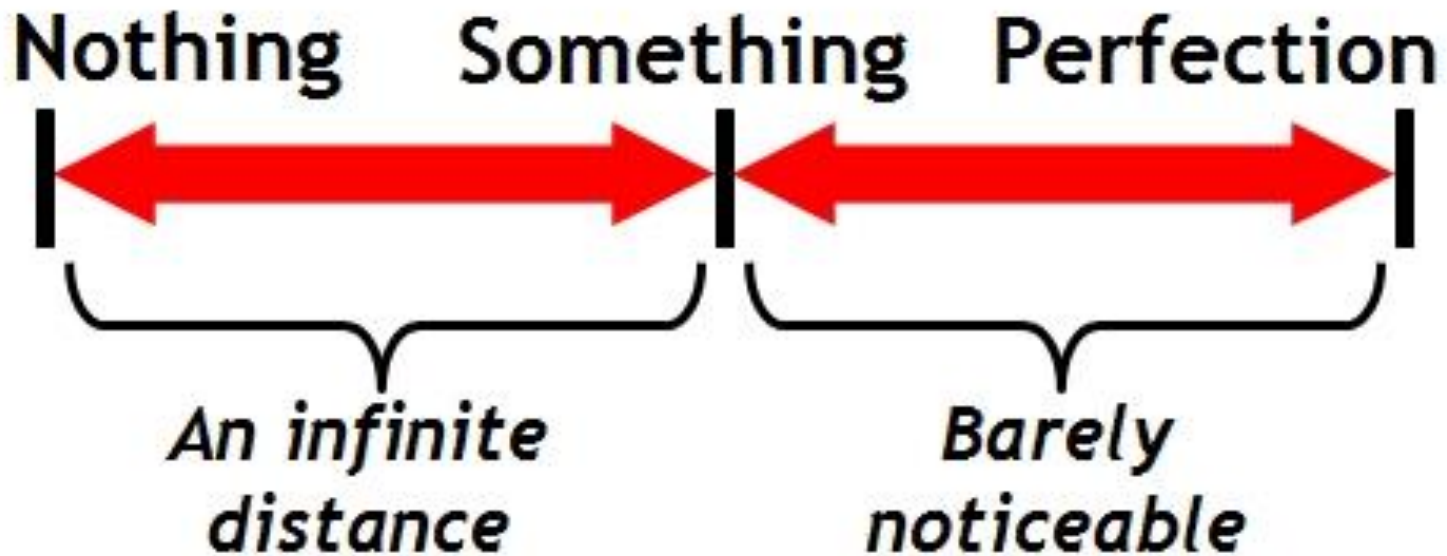


Digital Preservation Management:
Implementing Short-term Strategies for Long-term Problems

<http://www.dpworkshop.org/>

Building Digital Trust Statewide

REMEMBER THE GOLDEN RULE!



Building Digital Trust Statewide

THINK DIGITAL!



Building Digital Trust Statewide

**THE BEST LONG-TERM ARCHIVAL SOLUTION IS
SOUND RECORDS MANAGEMENT**





Thanks!

Jim Kichas
Utah State Archives
jkichas@utah.gov
801-531-3844